

CLERKS OFFICE U.S. DIST. COURT
AT LYNCHBURG, VA
FILED

4/25/2025

LAURA A. AUSTIN, CLERK
BY: s/ CARMEN AMOS
DEPUTY CLERK

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
LYNCHBURG ~~CHARLOTTESVILLE~~
DIVISION**

LILA WAKELEY, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

THRIVEWORKS ADMINISTRATIVE
SERVICES, LLC and THRIVEWORKS, INC.,

Defendants.

Case Number: 6:25CV0032

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Lila Wakeley (“Plaintiff”) brings this class action complaint individually and on behalf of all others similarly situated against Defendants Thriveworks Administrative Services, LLC and Thriveworks, Inc. (collectively, “Defendants” or “Thriveworks”). Plaintiff brings this action based on personal knowledge of the facts pertaining to herself, and on information and good faith belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF ACTION

1. This is a class action lawsuit brought on behalf of all Thriveworks patients who accessed mental health services on the website www.thriveworks.com (the “Website”).

Defendants purport to provide “award-winning therapy or psychiatry” online and in-person to children/teens, adults, couples, and families.¹

2. However, in pursuit of profit and without regard for their patients’ medical privacy, Defendants aid, employ, agree, and conspire with third parties LinkedIn Corporation (“LinkedIn”) and Google LLC (“Google”) to intercept patients’ communications as they seek

¹ <https://thriveworks.com/>

mental health services on the Website. This is achieved through Defendants' secret installation of complex computer code on the Website which serves to track and disclose Thriveworks patients' activity, in real time, to third parties LinkedIn and Google.

3. Imagine walking into a therapist's office, feeling a blend of hope and vulnerability. You fill out an intake form, honestly stating that you're seeking help for depression. This moment represents a significant step toward healing—a courageous decision to confront your struggles. The journey to get here hasn't been easy; you've navigated numerous barriers, including fear of stigma surrounding treatment, the challenge of opening up to a stranger, and the difficult realization that you need professional help.²

4. Later, you learn that from the moment you set foot in that office, the sensitive information about the care you are seeking was being shared beyond the walls of the therapist's office with unknown third parties. The very confidentiality you sought has been compromised, leaving you feeling exposed and betrayed.

5. Defendants' conduct does exactly that. By secretly disclosing Plaintiff's and Class members' sensitive and confidential medical information with third parties, Defendants undermined the importance of safeguarding the identities and personal medical information of individuals seeking therapy and breached its patients' trust—violating state and federal law.

6. When individuals seek therapy, they share sensitive personal information, including mental health history, personal struggles, and other confidential medical information. Data privacy is especially vital when booking therapy online, primarily due to the sensitive

² Hannah M. C. A. Verhoeven et al., *Understanding the Barriers to Mental Health Care: A Systematic Review of Qualitative Studies*, 10 Healthcare 228 (2022), <https://pmc.ncbi.nlm.nih.gov/articles/PMC9690172/pdf/healthcare-10-02228.pdf>.

nature of this protected medical information. When patients engage in therapy, they are legally entitled to protection from the unauthorized disclosure of their information to third parties.

7. When patients know their information is secure, as Defendants' claim,³ they are more likely to pursue the support they need without fear of judgment or exposure. This is particularly important in therapy, where societal stigma around mental health can already be a barrier to accessing care.

8. Information related to mental health treatment is protected by state and federal law, including but not limited to, the Health Insurance Portability and Accountability Act ("HIPAA") and the Virginia Health Records Privacy Act ("VHRPA"). Healthcare providers, like Thriveworks, are legally required to safeguard patients' health information. This means that any data related to a patient's mental health and treatment history, including patient status, must be kept confidential and secure. Given these protections, along with Defendants' representations, patients reasonably expect that information related to their mental health treatment will remain confidential.

9. Unbeknownst to Plaintiff and Class members, and contrary to Thriveworks' duties as a medical provider, Defendants disclose their patients' protected health information ("PHI") to third parties, including LinkedIn and Google, for targeted advertising purposes. This PHI includes, but is not necessarily limited to, the interactions patients take within their private patient portals and the specific therapy treatments they are seeking (e.g., addiction, postpartum depression, sexual abuse, etc.). Plaintiff brings this action for legal and equitable remedies resulting from Defendants' illegal actions.

³ <https://thriveworks.com/faq/>

THE PARTIES

10. At all relevant times, Plaintiff was a resident of Newtown Square, Pennsylvania. Plaintiff has been a patient of Thriveworks since 2023 and has made multiple appointments through its Website for mental health services.⁴ Plaintiff created her Thriveworks account using her Gmail account and booked her therapy appointments while logged into her patient portal. Plaintiff also watched prerecorded videos on the Thriveworks' Website located within her patient portal. These videos were provided by Thriveworks for the treatment of various mental health conditions. When scheduling her therapy appointments while logged into her patient portal on the Thriveworks Website, Plaintiff searched the conditions for which she was seeking treatment and provided information related to her health insurance. Plaintiff's last appointment with her therapist was scheduled through her patient portal on the Thriveworks Website on May 22, 2023.

11. Unbeknownst to Plaintiff, Defendants disclosed her PHI—including the specific reasons for which she was seeking therapy and information related to her health insurance provider—to LinkedIn and Google for targeted advertising purposes. Defendants also disclosed sufficient personally identifiable information ("PII") for LinkedIn and Google to identify Plaintiff as the specific individual booking her medical appointment, as described more thoroughly below.

12. After booking an appointment on the Thriveworks Website, Plaintiff began receiving targeted advertisements for similar products and services. Plaintiff would not have booked an appointment on the Website if she knew Defendants were violating her privacy by sharing her PHI with unknown third parties.

⁴ To prevent further disclosure of Plaintiff's confidential PHI, Plaintiff has not included in her allegations the precise nature of the treatment she received from Thriveworks.

13. At all relevant times Plaintiff has maintained both a LinkedIn and Gmail account. When registering for her LinkedIn account, LinkedIn required that she provide her full legal name, gender, and email account. When registering for her Gmail account, Google required that she provide her full legal name, date of birth, and gender. Every time Plaintiff accesses her Gmail account, Google collects information related to her IP address and electronic device (e.g. browser, operating system, screen resolution, etc.) and stores it in a profile maintained by Google for targeted advertising purposes. Google also utilizes other features, such as generating specific User IDs, to track its users across web browsing sessions for identification purposes, as detailed below. Google utilizes all of these tracking features in order to build robust consumer profiles it can then leverage for targeted advertising purposes. Plaintiff used the same device and browser to access the Thriveworks Website and both her LinkedIn and Gmail accounts.

14. Defendant Thriveworks Administrative Services, LLC is a Virginia limited liability company with its principal place of business located at 1000 Jefferson St., Ste. 2C, Lynchburg, Virginia. Defendant Thriveworks Administrative Services, LLC is a wholly owned subsidiary of Defendant Thriveworks, Inc. Defendant Thriveworks Administrative Services, LLC is a management services organization and maintains and operates the Website under the control and direction of Defendant Thriveworks, Inc.

15. Defendant Thriveworks, Inc. is a Virginia corporation with its principal place of business located at 1000 Jefferson St., Ste. 2C, Lynchburg, Virginia. Defendant Thriveworks, Inc. directs and controls the acts of Defendant Thriveworks Administrative Services, LLC to operate and maintain its Website, through which it offers mental health services to its patients.

16. Defendants maintain and operate the Website wherein their patients can seek and schedule appointments for mental health services and watch prerecorded videos for mental health

treatment for a variety of mental health conditions, including those related to anxiety, addiction, eating disorders, and divorce. Defendants chose to embed the LinkedIn Insight Tag and Google Analytics (the “Tracking Technologies”) on the Website, whereby they disclosed the confidential PHI of their patients with LinkedIn and Google for targeted advertising purposes. Defendants did this without authorization or consent from their patients.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff’s state law claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges that at least 100 people comprise the proposed class, that the combined claims of the proposed class members exceed \$5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from at least one defendant.

18. This Court has personal jurisdiction over Defendants because Defendants conduct substantial business within this District and Defendants reside in this District.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this claim occurred in this District and Defendants reside in this District.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

A. Health-Related Information is Sensitive and Confidential

20. Defendants assisted and enabled LinkedIn and Google, two of the largest data and technology companies in the world, with intercepting information that is sensitive, confidential, and personally identifiable.

21. Defendants operate the Website where their patients can access mental health services, including therapy appointments and prerecorded videos for the treatment of a wide array of mental health issues.

22. Under federal law, a healthcare provider may not disclose personally identifiable information (“PII”) or PHI without the patient’s express written authorization.⁵ In this case, PHI includes, but is not necessarily limited to, patient status, mental health conditions, and information related to therapy appointments, including the specialty sought by the patient (i.e. addiction, eating disorder, depression, etc.).

23. The United States Department of Health and Human Services (“HHS”) has established a national standard, known as the HIPAA Privacy Rule, to explain the duties healthcare providers owe to their patients. “The Rule requires appropriate safeguards to protect the privacy of [PHI] and sets limits and conditions on the uses and disclosures that may be made of such information without an individual’s authorization.”⁶

24. A healthcare provider violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-d9 (“Part C”): “(1) uses of causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.”⁷

25. The statute states that an entity “shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity...and the individual obtained or disclosed such information without authorization.” *Id.*

⁵ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

⁶ U.S. Dept. of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>.

⁷ 42 U.S.C. § 1320d-6.

26. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendants because they are knowingly disclosing individually identifiable health information relating to their patients.

27. Defendants further failed to comply with other HIPAA safeguard regulations as follows:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants created, received, maintained and transmitted in violation of 45 C.F.R. Section 164.306(a)(1);
- b. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. Section 164.308(a)(1);
- c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendants in violation of 45 C.F.R. Section 164.308(a)(6)(ii);
- d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. Section 306(a)(2);
- e. Failing to protect against reasonably anticipated uses of disclosures of electronic PHI not permitted under privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. Section 164.306(a)(3); and
- f. Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably

safeguard PHI in violation of 45 C.F.R. Section 164.530(c).

28. Health care organizations regulated under HIPAA, like Defendants, may use third-party tracking tools in a limited way to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to vendors (as shown below). As explained by a statement published by the HHS:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. **For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.**⁸

29. The Bulletin discusses the types of harm that disclosure may cause to the patient:

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.**⁹

⁸ HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (THE "BULLETIN") (EMPHASIS ADDED), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

⁹ *Id.* (emphasis added).

30. Plaintiff and Class members face exactly the risks over which the government expresses concern. Defendants' unlawful conduct resulted in third parties intercepting information regarding Plaintiff and Class members' mental health treatments when logged into their patient portal on Defendants' Website.

31. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

This information might include an individual's medical record number, home or email address, or **dates of appointments**, as well as **an individual's IP address** or geographic location, medical device IDs, **or any unique identifying code**.¹⁰

32. Crucially, the Bulletin continues:

All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, **such as IP address** or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus **relates to the individual's past, present, or future health or health care or payment for care**.¹¹

33. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking

¹⁰ *Id.* (emphasis added).

¹¹ *Id.* (emphasis added).

technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.

“When consumers visit a hospital’s [regulated entity’s] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties,” said Samuel Levine, Director of the FTC’s Bureau of Consumer Protection. “The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers’ health information from potential misuse and exploitation.”

“Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital’s [regulated entity’s] website,” said Melanie Fontes Rainer, OCR Director. “OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue.”

The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user’s online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.

In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual’s personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, **medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.**¹²

¹² Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>. (emphasis added).

34. The FTC is unequivocal in its stance. The FTC has specifically informed healthcare companies, like Defendants, that they should not use tracking technologies to collect sensitive health information and disclose it to third party advertising platforms without informed consent:

The FTC Act prohibits companies and individuals from engaging in unfair or deceptive acts or practices in or affecting commerce. This means you must ensure your health data practices aren't substantially injuring consumers, including by invading their privacy.

For instance, *BetterHelp*, *GoodRx*, and *Premom* make clear that disclosing consumers' health information for advertising without their affirmative express consent may be an unfair practice.

[I]f you use behind-the-scenes tracking technologies that share consumers' sensitive health data in contradiction of your privacy promises, that's a violation of the FTC Act.¹³

35. Therefore, Defendants' conduct, as described herein, is directly contrary to federal law and the clear pronouncements by the FTC and HHS.

B. LinkedIn's Advertising Technology

36. LinkedIn markets itself as "the world's largest professional network on the internet[.]"¹⁴ But LinkedIn is no longer simply a tool to help users find jobs or expand their professional network. LinkedIn has moved into the marketing and advertising space and boasts of its ability to allow potential advertisers to "[r]each 1 billion+ professionals around the world" via its Marketing Solutions services.¹⁵ Recently, LinkedIn was projected as being responsible

¹³ <https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach>

¹⁴ LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?, <https://www.linkedin.com/help/linkedin/answer/a548441#>.

¹⁵ LINKEDIN, MARKETING SOLUTIONS, <https://business.linkedin.com/marketing-solutions>.

for “roughly 0.9 percent of the global ad revenue” which included approximately \$5.91 billion in advertising revenue in 2022.¹⁶

37. According to LinkedIn, “[t]argeting is a foundational element of running a successful advertising campaign — [g]etting your targeting right leads to higher engagement, and ultimately, higher conversion rates.”¹⁷ Targeting refers to ensuring that advertisements are targeted to, and appear in front of, the target demographic for an advertisement. To that end, LinkedIn’s Marketing Solutions services allow potential advertisers to “[b]uild strategic campaigns” targeting specific users.¹⁸ LinkedIn’s “marketing solutions allow advertisers to select specific characteristics to help them reach their ideal audience. The ads [users] see on LinkedIn are then targeted to provide content relevant to [the users].”¹⁹

38. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals’ demographics, intent, behavior, engagement, interests, buying decisions, and more.²⁰

39. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn’s Marketing Solutions including Ad Targeting,

¹⁶ Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023), <https://www.statista.com/statistics/275933/linkedin-advertising-revenue>.

¹⁷ LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3, <https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf>.

¹⁸ LINKEDIN, *supra* note 11.

¹⁹ LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS, <https://www.linkedin.com/help/lms/answer/a421454>.

²⁰ See LINKEDIN, MARKETING SOLUTIONS, <https://business.linkedin.com/marketing-solutions/audience> (“Target audiences through demographic marketing[,]” “Zero in on intent, behavior, engagement, interests, and more[,]” and “Reach the LinkedIn audience involved in the buying decision”).

Matched Audiences, Audience Expansion, Predictive Audience, and LinkedIn Audience Network.²¹

40. Such information is extremely valuable to marketers and advertisers because the inferences derived from users' personal information and communications allow marketers and advertisers, including healthcare providers and insurance companies, to target potential customers.²²

41. For example, through the use of LinkedIn's Audience Network, marketers and advertisers are able to expand their reach and advertise on sites other than LinkedIn to "reach millions of professionals across multiple touchpoints."²³ According to Broc Munro of Microsoft, "[w]e gravitate towards social platforms like LinkedIn to achieve more targeted marketing engagement. However, we know that our audiences don't spend all their time on social media. LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting our audience targeting. This increases the impact of our advertising."²⁴

²¹ *See id.*

²² LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy> ("We serve you tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you cannot opt-out of seeing other ads."); LINKEDIN, ACCOUNT TARGETING, <https://business.linkedin.com/marketing-solutions/ad-targeting> ("Target your ideal customer based on traits like their job title, company name or industry, and by professional or personal interests"); LINKEDIN, EXAMPLES OF TRENDING AND BEST-IN-CLASS HEALTHCARE CAMPAIGNS AND CONTENT, p.6, <https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf> ("BD zeroed in on the end-benefit with a 30 second video introducing their PIVO needle-free blood collection device to potential customers."); LINKEDIN, HEALTHCARE SOCIAL MEDIA STRATEGIES FOR 2023, p.1, <https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf> (listing "potential customers" as "Common audiences" for insurance sector).

²³ LINKEDIN, ACCOUNT TARGETING, <https://business.linkedin.com/marketing-solutions/ad-targeting>.

²⁴ LINKEDIN, LINKEDIN AUDIENCE NETWORK, <https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network>.

42. In July 2022, “LinkedIn Marketing Solutions surpassed \$5 billion in annual revenue[.]”²⁵ That figure is “expected to further grow to reach 10.35 billion U.S. dollars by 2027.”²⁶

43. According to LinkedIn, the LinkedIn Insight Tag is “[a] simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget your website visitors, and learn more about your audiences.”²⁷ LinkedIn represents that the LinkedIn Insight Tag “enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors.”²⁸

44. LinkedIn’s current iteration of its Insight Tag is a JavaScript-based code which allows for the installation of its software.²⁹ A critical feature allows the LinkedIn Insight Tag to track users, even when third-party cookies are blocked.³⁰ LinkedIn “recommend[s] using the JavaScript-based Insight Tag or Conversions API” because third-party cookie settings are being deprecated across the industry.³¹ Embedding the JavaScript as a first-party cookie causes users’ browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited,

²⁵ *LinkedIn Business Highlights from Microsoft’s FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July 25, 2022), <https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time>.

²⁶ Dencheva, *supra* note 12.

²⁷ LINKEDIN, INSIGHT TAG, <https://business.linkedin.com/marketing-solutions/insight-tag>.

²⁸ LINKEDIN, LINKEDIN INSIGHT TAG FAQs, <https://www.linkedin.com/help/lms/answer/a427660>.

²⁹ LINKEDIN, *supra* note 22.

³⁰ *Id.* (“It’s important for advertisers to prepare for these changes by switching to JavaScript tags and enabling ‘enhanced conversion tracking’ in the Insight Tag settings to continue capturing signals where 3rd party cookies are blocked.”).

³¹ *See id.*

rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of modern web browsers do not prevent LinkedIn from collecting data through its software.³² Instead, the LinkedIn Insight Tag is shielded with the same privacy exemptions offered to first-party cookies.

45. When a user who has signed in to LinkedIn (even if the user subsequently logs out) is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent using cookies, which includes information about the user's actions on the website.

46. These cookies also include data that differentiate users from one another and can be used to link the data collected to the user's LinkedIn profile.

47. The HTTP request about an individual who has previously signed into LinkedIn includes requests from the "li_sugr" and "lms_ads" cookies. Each of these cookies are used by LinkedIn "to identify LinkedIn Members off LinkedIn" for advertising purposes.³³

48. For example, the "li_sugr" cookie is "[u]sed to make a probabilistic match of a user's identity."³⁴ Similarly, the "lms_ads" cookie is "[u]sed to identify LinkedIn Members off LinkedIn for advertising."³⁵

49. A LinkedIn profile contains information including an individual's first and last name, place of work, contact information, and other personal details. Based on information it obtains through the LinkedIn Insight Tag, which Defendants installed on the Website, LinkedIn is able to target its account holders for advertising.

³² *See id.*

³³ LINKEDIN, LINKEDIN COOKIE TABLE, <https://www.linkedin.com/legal/l/cookie-table>.

³⁴ *See id.*

³⁵ *See id.*

50. LinkedIn never receives consent from users to intercept and collect electronic communications containing their sensitive and unlawfully disclosed information. In fact, LinkedIn expressly warrants the opposite. Similarly, Defendants never receive consent from their patients to share information with LinkedIn.

51. When first signing up, a user agrees to the User Agreement.³⁶ By using or continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy Policy³⁷ and the Cookie Policy.³⁸

52. LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect the world's professionals Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared."³⁹

53. The Privacy Policy goes on to describe what data LinkedIn collects from various sources, including cookies and similar technologies.⁴⁰ LinkedIn states "we use cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services. We also allow some others to use cookies as described in our Cookie Policy."⁴¹

54. However, LinkedIn offers an express representation: "**We will only collect and process personal data about you where we have lawful bases.**"⁴²

³⁶ LINKEDIN, USER AGREEMENT, <https://www.linkedin.com/legal/user-agreement>.

³⁷ LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy>.

³⁸ LINKEDIN, COOKIE POLICY, <https://www.linkedin.com/legal/cookie-policy>.

³⁹ LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy>.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.* (emphasis added).

55. Users never choose to provide sensitive information to LinkedIn because, among other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if so, what sensitive personal data it collects.

C. Google's Advertising Technology

56. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each device (such as a computer, tablet, laptop, or smartphone) accesses web content through a web browser (e.g. Chrome, Safari, Edge, etc.).

57. Every website is hosted by a computer server that holds the website's contents and through which the entity in charge of the website exchanges communications with the consumer's device via web browsers.

58. Web communications consist of HTTP Requests and HTTP Responses and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- HTTP Request: an electronic communication sent from a device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- Cookies: a small text file that can be used to store information on the device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- HTTP Response: an electronic communication that is sent as a reply to the device's web browser from the host server in response to a HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

59. A consumers' HTTP Request essentially asks the Website to retrieve certain

information (such as appointment booking information), and the HTTP Response renders or loads the requested information in the form of “Markup” (the pages, images, words, buttons, and other features that appear on the consumer’s screen as they navigate the Website).

60. Every website is comprised of Markup and “Source Code.” Source Code is a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code.

61. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser’s user. The Tracking Technologies embedded on the Website by Defendants constitute Source Code and function in a substantially similar way.

62. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over \$1 trillion dollars. Google fancies itself a “tech” company, but Google, at its core, is an advertising company.

63. Google “make[s] money” from “advertising products [that] deliver relevant ads at just the right time,” generating “revenues primarily by delivering both performance advertising and brand advertising.”⁴³ In 2020, Google generated \$146.9 billion in advertising revenue, which amounted to more than 80 percent of Google’s total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

Figure 1:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	\$257.6 billion	\$209.5	81.33%
2020	\$182.5 billion	\$146.9 billion	80.49%
2019	\$161.9 billion	\$134.8 billion	83.29%
2018	\$136.8 billion	\$116.5 billion	85.12%

⁴³ ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm>.

64. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google's SDK and pixel integrate with Google's advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google's ad network and products increasing Google's overall ad revenue. Products like Google's SDK and its tracking pixel also improve the company's advertising network and capabilities by providing more wholesome profiles and data points on individuals.

65. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

66. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth information about user behavior. Also, Universal Analytics enabled tracking the same user across multiple devices through its addition of the User-ID feature, which "associate[s] a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices."

67. In 2020, Google launched Google Analytics 4, a platform combining Google Analytics with Firebase to analyze both app and web activity.

68. Since launching Google Analytics, Google has become one of the most popular web analytics platforms on the internet. Indeed, Google had a \$62.6 billion increase in

advertising revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

69. Google touts Google Analytics as a marketing platform that offers “a complete understanding of your customers across devices and platforms.”⁴⁴ It allows companies and advertisers that utilize it to “understand how your customers interact across your sites and apps, throughout their entire lifestyle,” “uncover new insights and anticipate future customer actions with Google’s machine learning to get more value out of your data,” “take action to optimize marketing performance with integrations across Google’s advertising and publisher tools,” and “quickly analyze your data and collaborate with an easy-to-use interface and shareable reports.”⁴⁵

70. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site—even when Thriveworks patients are logged into their patient portals. This code immediately intercepts a user’s interaction with the webpage every time the user visits it, including what pages they visit and what they click on. The code also collects PII, such as IP addresses and device information related to the specific computing device a consumer (or patient) is using to access a website. The device information intercepted by Google includes the patient’s operating system, operating system version, browser, language, and screen resolution.

71. In other words, when interacting with the Website, an HTTP Request is sent to Thriveworks’ server, and that server sends an HTTP Response including the Markup that

⁴⁴ *Analytics*, GOOGLE, <https://marketingplatform.google.com/about/analytics/> (last visited Jan. 10, 2023).

⁴⁵ *Id.*

displays the website visible to the patient and Source Code, including Google's Tracking Technologies.

72. Thus, Defendants are essentially handing their patients a tapped device, and once the webpage is loaded onto the patient's browser, the software-based wiretap is quietly waiting for private communications on the Website to trigger the tap, which intercepts those communications intended only for Defendants and transmits those communications to third parties like Google.

73. Once Google's software code collects the data intercepted from the Website, it packages the information and sends it to Google Analytics for processing. Google Analytics enables the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google Analytics database and cannot be changed.

74. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on acquisition (e.g., information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (e.g., classify your users by age, location, language, and gender, along with interests they express through their online browsing and purchase activities).

75. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

76. The Website utilizes Google's pixel and SDK. As a result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least "Custom Events" and URLs that disclosed the mental health services being received by the patient. Google also received additional PII, including the patients' IP address, device information, and User-IDs.

77. For example, the Website utilizes Google's "cid" or "Client ID" function to identify patients as they navigate the Website.⁴⁶

78. In addition to User-IDs, upon receiving information from the Website, Google also utilizes a "browser-fingerprint" to personally identify consumers. A browser-fingerprint is information collected about a computing device that is used to identify the specific device.

79. These browser-fingerprints are used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data.

80. As Google explained, "[w]ith fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."⁴⁷

81. The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it

⁴⁶ [https://www.owox.com/blog/use-cases/google-analytics-client-id#:~:text=The%20Client%20ID%20\(cid\)%20or,unique%20users%20using%20this%20parameter.](https://www.owox.com/blog/use-cases/google-analytics-client-id#:~:text=The%20Client%20ID%20(cid)%20or,unique%20users%20using%20this%20parameter.)

⁴⁷ <https://www.blog.google/products/chrome/building-a-more-private-web/>

employs much more subtle techniques.⁴⁸ Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.

82. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.⁴⁹

83. Browser-fingerprints are personal identifiers. Google Analytics can collect browser-fingerprints from website visitors.

84. As enabled by Defendants, Google collects vast quantities of consumer data through Google Analytics.

85. Due to the vast network of consumer information held by Google, it is able to match the IP addresses, device information, and User-IDs it intercepts and link such information to an individual's specific identity.

86. Google then utilizes such information for its own purposes, such as targeted advertising.

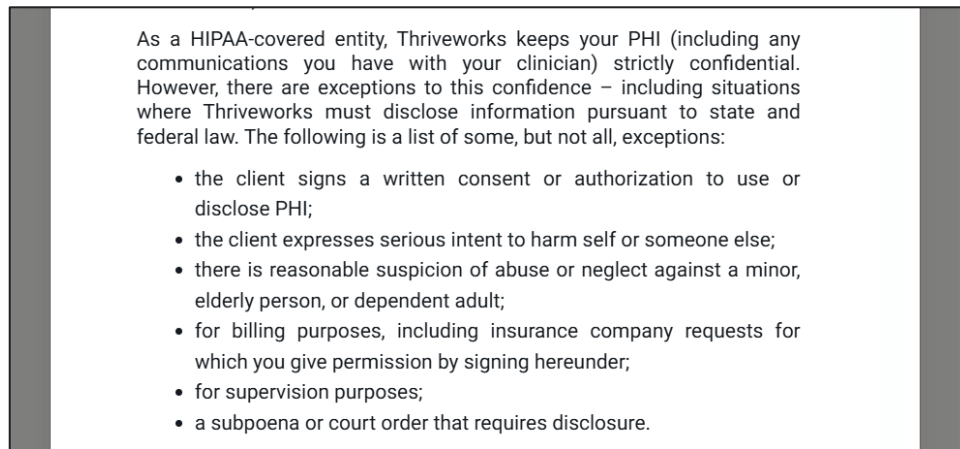
D. Thriveworks Violates the Privacy Rights of its Patients

42. Thriveworks is an online healthcare provider that connects patients with therapists and psychiatrists. Upon entering the Website, Thriveworks warrants that it will help its patients “[g]et award-winning therapy or psychiatry, covered by insurance.”

43. Defendants understand that the information handled on the Thriveworks Website is protected and confidential. For example, Defendants make the following warranty to their patients when they register an account on the Website:

⁴⁸ <https://www.pixelprivacy.com/resources/browser-fingerprinting/>

⁴⁹ <https://ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/>

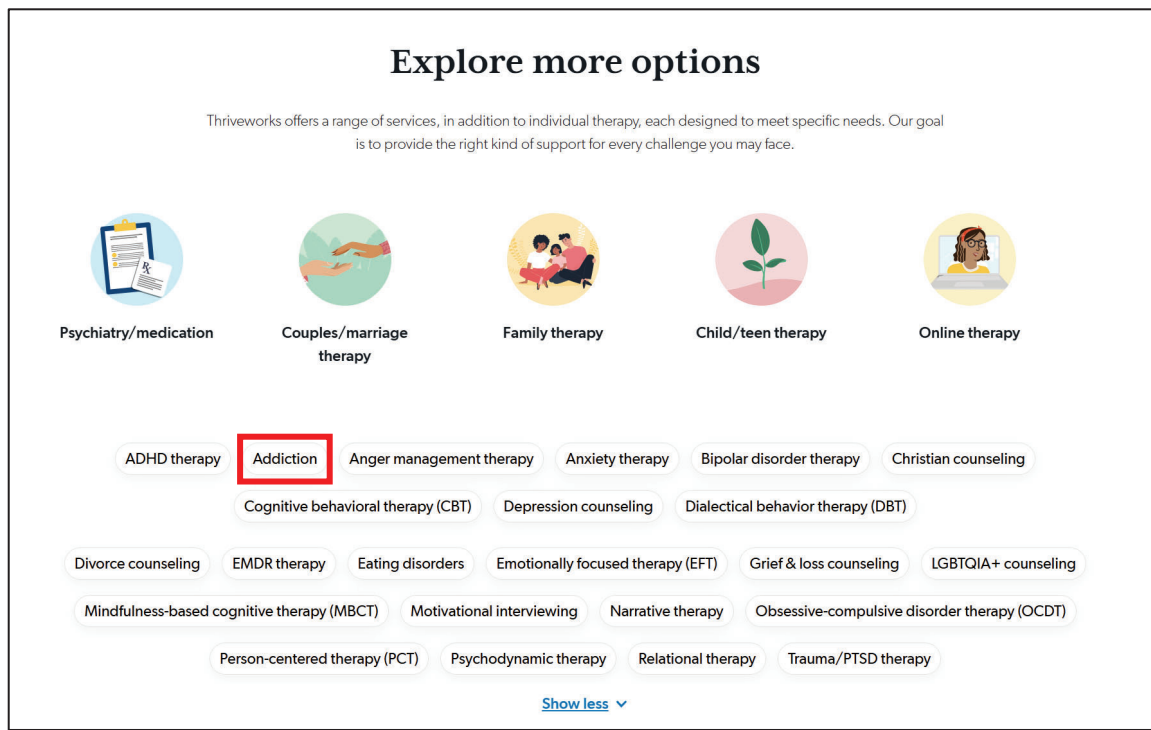
Figure 2:

44. Unfortunately, Thriveworks does not comply with its obligations and representations.

45. Defendants allow their patients to access mental health services on the Website, including booking therapy appointments and accessing prerecorded videos for mental health treatment.

46. Unbeknownst to their patients, Defendants embedded the Tracking Technologies onto the Website, including after patients have logged into their account portals, to search and schedule therapy appointments and watch prerecorded videos for mental health treatment.

47. For example, patients can search for and schedule therapy appointments for several different mental health conditions on the Thriveworks Website. When patients select a condition for which they would like to receive treatment, Defendants disclose this information to LinkedIn:

Figures 3-4:

▼ Request Payload view source

```
{
  "pids": [4112044],
  "scriptVersion": 199,
  "time": 1744978659100,
  "domain": "thriveworks.com",
  "domAttributes": {
    "elementSemanticType": null,
    "elementValue": null,
    "elementType": null,
    "tagName": "A",
    "domain": "thriveworks.com"
  },
  "elementCrumbsTree": [
    {
      "tagName": "div",
      "nthChild": 1,
      "id": "page-container"
    },
    {
      "tagName": "div",
      "nthChild": 1,
      "id": "main-area"
    }
  ],
  "hem": null,
  "href": "https://thriveworks.com/app/providers?&areaOfConcern%5B%5D=75edbd3e-f37e-435a-909a-11463be88086",
  "innerElements": null,
  "isFilteredByClient": false,
  "isLinkedInApp": false,
  "isTranslated": false,
  "liFatId": "",
  "liGiant": "",
  "misc": {
    "nsbState": -4
  },
  "pageTitle": "Book an Addiction Counseling Appointment",
  "pids": [4112044],
  "scriptVersion": 199,
  "signalType": "CLICK",
  "url": "https://thriveworks.com/find-help/addiction-counseling/",
  "websiteSignalRequestId": "2b695d94-1a3a-2bfb-e6c8-be3f0bc178f3"
}
```

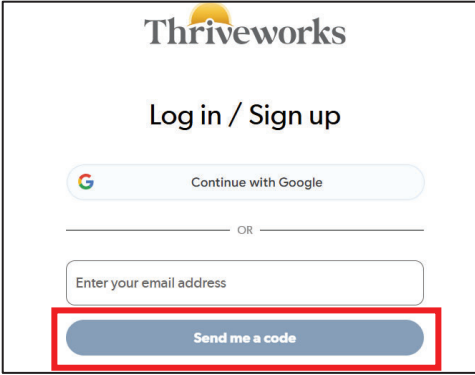
48. The information disclosed by Defendants were accompanied by the lms_ads and li_sugr cookies, whereby LinkedIn could connect the disclosed PHI with the patients' PII.

49. The information shared by Defendants allows LinkedIn to know the identities of specific individuals as well as information related to the mental health treatment they are

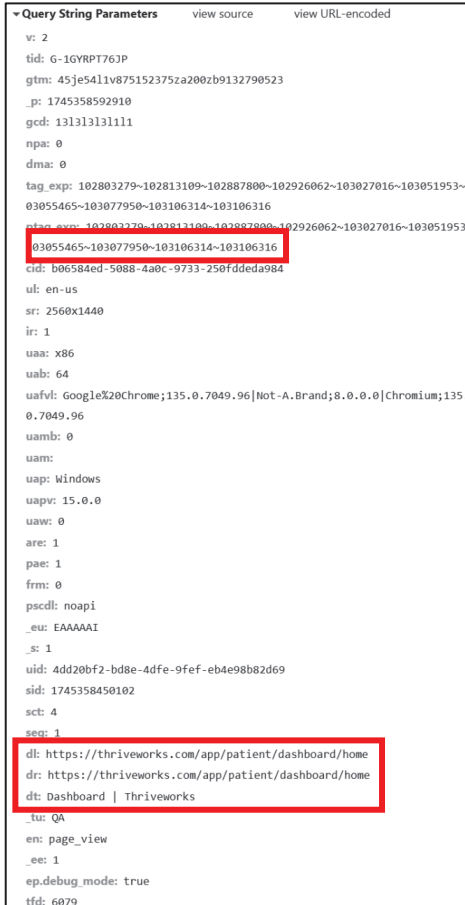
receiving. This allows these companies, including Defendants, to profit from this information for targeted advertising purposes.

50. Defendants make similar disclosures to Google. For example, when a patient logs into their patient portal, Defendants disclose this information to Google:

Figures 5-6:



The image shows the Thriveworks login and sign-up page. At the top is the Thriveworks logo. Below it is the text "Log in / Sign up". There is a "Continue with Google" button with the Google logo. Below that is a horizontal line with "OR" in the center. Underneath is a text input field labeled "Enter your email address". At the bottom is a blue button labeled "Send me a code", which is highlighted with a red rectangular box.

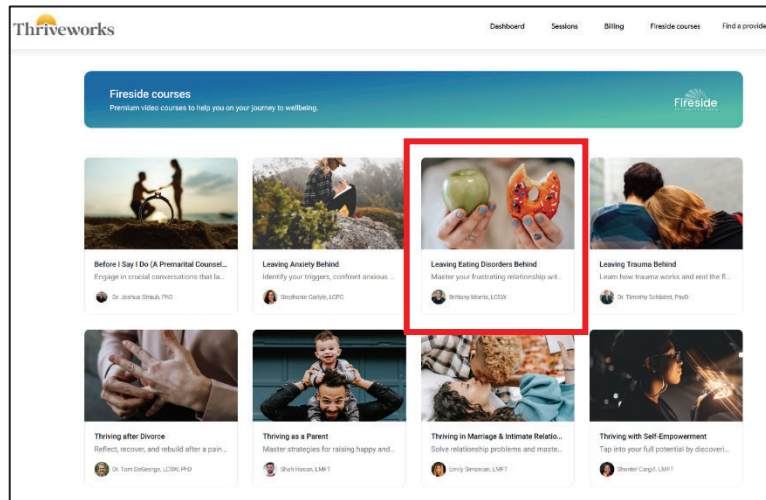


The image shows a list of query string parameters from a web browser's developer tools. The parameters are listed in a text area. Two specific parameters are highlighted with red rectangular boxes: "cid: 03055465~103077950~103106314~103106316" and "dt: Dashboard | Thriveworks".

```
▼ Query String Parameters view source view URL-encoded
v: 2
tid: G-1GYRPT763P
gtm: 45je5411v875152375za200zb9132790523
_p: 1745358592910
gcd: 13131313111
npa: 0
dma: 0
tag_exp: 102803279~102813109~102887800~102926062~103027016~103051953~
03055465~103077950~103106314~103106316
cid: 03055465~103077950~103106314~103106316
cid: b06584ed-5088-4a0c-9733-250fddeda984
ul: en-us
sr: 2560x1440
ir: 1
uaa: x86
uab: 64
uafv: GoogleX20Chrome;135.0.7049.96|Not-A.Brand;8.0.0|Chromium;135.
0.7049.96
uamb: 0
uam:
uap: Windows
uapv: 15.0.0
uaw: 0
are: 1
pae: 1
frm: 0
pscd: noapi
_eu: EAAAAAI
_s: 1
uid: 4dd20bf2-bd8e-4dfe-9fef-eb4e98b82d69
sid: 1745358450102
sct: 4
seq: 1
dl: https://thriveworks.com/app/patient/dashboard/home
dr: https://thriveworks.com/app/patient/dashboard/home
dt: Dashboard | Thriveworks
_tu: QA
en: page_view
_ee: 1
ep.debug_mode: true
tfd: 6079
```

51. Once logged into their patient portal, similar disclosures are made when patients search for and view prerecorded videos for the treatment of mental health conditions:

Figures 7-8:



▼ Query String Parameters view source view URL-encoded

```
v: 2
tid: G-8ZVFM98QD
gtm: 45je5411v9132790523za200
_p: 1745358946426
gcd: 13131313111
npa: 0
dma: 0
tag_exp: 102803279~102813109~102887800~102926062~103027016~103051953~103055465~103077950~103106314~103106316
cid: b06584ed-5088-4a0c-9733-250fddeda984
ul: en-us
sr: 2560x1440
uaa: x86
uab: 64
uafvl: Google%20Chrome;135.0.7049.96|Not-A.Brand;8.0.0.0|Chromium;135.0.7049.96
uamb: 0
uam:
uap: Windows
uapv: 15.0.0
uaw: 0
are: 1
frm: 0
pscdl: noapi
_eu: AEAAAAI
_s: 2
uid: 4dd20bf2-bd8e-4dfe-9fef-eb4e98b82d69
sid: 1745358450102
dl: https://thriveworks.com/app/patient/dashboard/fireside/leaving-eating-disorders-behind/eating-disorders-disordered-eating-trailer
dr: https://thriveworks.com/app/patient/dashboard/home
sec: 4
seg: 1
dt: Fireside | Thriveworks
_tu: QA
en: page_view
ep.debug_mode: true
_et: 4321
up.userId: patient
up.internal: false
tfd: 10198
```

52. Finally, Defendants disclose to Google when its patients' schedule therapy appointments:

Figures 9-10:

▼ Query String Parameters view source view URL-encoded

v: 2
tid: G-1GYRPT76JP
gtm: 45je54l0v875152375za200
_p: 1745406075744
gcd: 13l3l3l3l1l1
npa: 0
dma: 0
tag_exp: 102803279~102813109~102887800~102926062~103027016~103051953~103055465~103077950~103106314~103106316
cid: b06584ed-5088-4a0c-9733-250fddeda984
ul: en-us
sr: 2560x1440
ir: 1
uaa: x86
uab: 64
uafvl: Google%20Chrome;135.0.7049.96|Not-A.Brand;8.0.0.0|Chromium;135.0.7049.96
uamb: 0
uam:
uap: Windows
uapv: 15.0.0
uaw: 0
are: 1
pae: 1
frm: 0
pscdl: noapi
_eu: EEAAAAI
_s: 2
uid: 4dd20bf2-bd8e-4dfe-9fef-eb4e98b82d69
sid: 1745404363015
dl: https://thriveworks.com/app/providers?latitude=25.7616798&longitude=-80.1917902&state=FL&location=Miami,%20FL,%20USA&limit=10&offset=0&counselingType[]=fa040321-294c-4d0a-8c05-ac94a3797697
dr: https://thriveworks.com/app/providers
sct: 7
seg: 1
dt: Thriveworks Counseling - Find and Book sessions with Providers
_tu: QA
en: page_view
ep.debug_mode: true
_et: 1214
up.userId: patient

```
▼ Query String Parameters    view source    view URL-encoded

v: 2
tid: G-8ZVFM98QD
gtm: 45je5410v9132790523za200zb875152375
_p: 1745405224344
gcd: 13131313111
npa: 0
dma: 0
tag_exp: 102803279~102813109~102887800~102926062~103027016~103051953~1
03055465~103077950~103106314~103106316
ptag_exp: 102803279~102813109~102887800~102926062~103027016~103051953~
103055465~103077950~103106314~103106316
cid: b06584ed-5088-4a0c-9733-250fddeda984
ul: en-us
sr: 2560x1440
uaa: x86
uab: 64
uafvl: Google%20Chrome;135.0.7049.96|Not-A.Brand;8.0.0|Chromium;135.
0.7049.96
uamb: 0
uam:
uap: windows
uapv: 15.0.0
uaw: 0
are: 1
frm: 0
pscdl: noapi
_eu: AEAIAAI
_s: 5
uid: 4dd20bf2-bd8e-4dfe-9fef-eb4e98b82d69
sid: 1745404363015
dl: https://thriveworks.com/app/bookings/user/payment?tz=America%2FNew
_York&slotId=d522383d-da4e-435b-bf81-84ccefc5528d
dr: https://thriveworks.com/app/bookings/user/patient-info?tz=America%
2FNew_York&slotId=d522383d-da4e-435b-bf81-84ccefc5528d
sct: 8
seg: 1
dt: Payment - Booking | Thriveworks
_tu: QA
en: page_view
```

53. Finally, when patients are scheduling their therapy appointments, Defendants disclose this information to Google, including the specific conditions the patient is seeking treatment for and the patient's insurance carrier:

Figures 11-13:

The screenshot shows a patient portal interface. At the top, there are filters for Location (Miami, FL, USA), Specialty (Sexual Abuse, Postpar...), and Insurance (My insurance is...). Below these are buttons for 'Counseling' and 'Visit type'. A 'Search specialties' dropdown menu is open, displaying a list of specialties with checkboxes. The following specialties are listed: Narcissism, OCD / Obsessive-Compulsive, Postpartum / Pregnancy (checked and highlighted with a red box), Psychological Testing, Self Esteem, Self Harm, Sex Therapy, and Sexual Abuse (checked and highlighted with a red box). In the background, a calendar for April 24-27 is visible, showing appointment slots for 12 pm.

areaOfConcern[]=16ae3882-3b63-4890-b30d-dc4981e779ae
areaOfConcern[]=2f3e8f62-a2dc-42d7-84dc-aac9f6f2c422

Sexual Abuse = areaOfConcern[]=16ae3882-3b63-4890-b30d-dc4981e779ae
Postpartum = areaOfConcern[]=2f3e8f62-a2dc-42d7-84dc-aac9f6f2c422

54. During this process, Thriveworks assigns unique values to the selections made by its patients when sending the information to Google. However, Google can and does know the meaning behind the values disclosed by Thriveworks. The same is true when a patients provides information related to other mental health conditions, their counseling type, their appointment mode, their gender, and their insurance carrier.

55. Defendants further assist Google by disclosing the PII of its patients sufficient for Google to uncover their identities. In both HTTP communications, like Figures 6, 8-10, and 12-13, the patient's IP address is inherently included in every network request. In addition to its patients' IP addresses, Defendants, through Google Analytics, disclosed information about their

specific devices and User-IDs to Google, allowing Google to link such information to an individual's specific identity.

56. As shown above, Plaintiff's communications with Defendants were disclosed by Defendants to Google and/or intercepted in transit by Google, in real time, via detailed URLs, which contain the medically sensitive information and personally identifiable information entered into the Website.

57. Defendants also use and cause the disclosure of data sufficient for Google to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning mental health services.

58. Defendants sent these identifiers (e.g. cid, IP address, and device information) with each patient's "event" data.

59. Such event data includes the fact that a patient is seeking medical treatment (i.e. mental health services) and whether the patient is logged into their patient portal. *See* Figures 8-10.

60. When patients share their personal information with medical professionals, they expect this information to be kept confidential. Moreover, when consumers seek a specific treatment from medical professionals, they also expect this highly sensitive information to be kept confidential.

61. If patients knew that Defendants were sharing their personal information for targeted advertising purposes, they would seek treatment with another company. Through the above-listed third party tracking services, which Defendants used via the software code installed, integrated and embedded into the Website, Defendants disclosed their patients' legally protected PII and PHI.

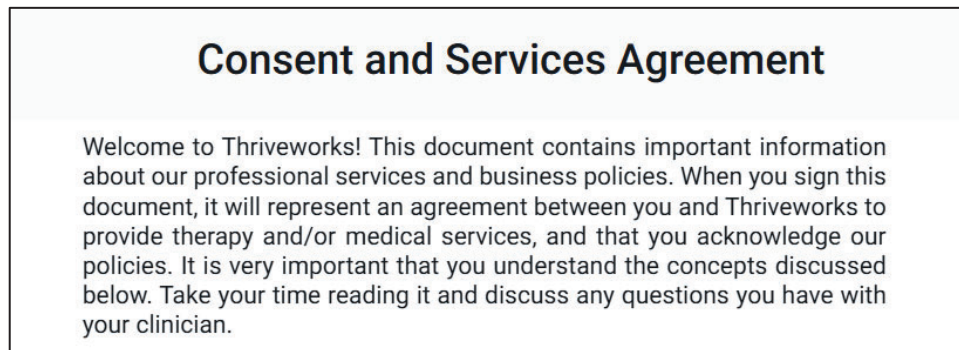
62. By installing, integrating and embedding the above-listed Tracking Technologies into the Website, and by directing such installation, integration and embedding, Defendants aided and conspired with the third parties and others to allow those third-party entities to contemporaneously and surreptitiously intercept the Website communications of Defendants' patients without the patient's consent.

63. Defendants engage in this deceptive conduct for their own profit at the expense of their patients' privacy. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violate federal and state law.

E. Thriveworks' Consent and Services Agreement

64. When patients complete their enrollment on Defendants' platform they must agree to and sign a Consent and Services Agreement:

Figure 14:



65. Pursuant to the Consent and Services Agreement, Thriveworks represents to its patients that it is "governed by the laws of the state in which you are located when receiving services. Where this...Agreement differs from relevant state or federal laws, those laws will govern."

66. Thriveworks also represents that it will protect its patients' PHI, as shown in Figure 2.

F. Tolling of Claims

67. Any applicable statutes of limitations have been tolled by Defendants' knowing and active concealment of its incorporation of the Tracking Technologies into its Website.

68. The Tracking Technologies were and are entirely invisible to a website visitor.

69. Through no fault or lack of diligence, Plaintiff and Class members were deceived and could not reasonably discover Defendants' deception and unlawful conduct.

70. Plaintiff was ignorant of the information essential to pursue her claims, without any fault or lack of diligence on her part.

71. Defendants had exclusive knowledge that its Website incorporated the Tracking Technologies and yet failed to disclose to its patients, including Plaintiff and Class members, that by accessing mental health services through the Website, including within their private patient portals, Plaintiff's and Class members' PHI would be disclosed or released to LinkedIn and Google.

72. Under the circumstances, Defendants were under a duty to disclose the nature, significance, and consequences of its collection and treatment of its patients' PHI. In fact, to the present, Defendants have not conceded, acknowledged, or otherwise indicated to its patients that it disclosed or released their PHI to unauthorized third parties. Accordingly, Defendants are estopped from relying on any statute of limitations.

73. Moreover, all applicable statutes of limitations have also been tolled pursuant to the discovery rule.

74. The earliest that Plaintiff or Class members, acting with due diligence, could have reasonably discovered Defendants' conduct would have been shortly before the filing of the Plaintiff's complaint in this matter.

75. Plaintiff first discovered that Defendants had collected and disclosed her PHI to LinkedIn and Google on or around April 2025 after contacting undersigned counsel.

CLASS ACTION ALLEGATIONS

76. Plaintiff brings this action on behalf of all persons in the United States who accessed their patient portal on www.thriveworks.com for mental health services (the “Class”).

77. Plaintiff also brings this action on behalf of all persons in Pennsylvania who accessed their patient portal on www.thriveworks.com for mental health services (the “Pennsylvania Subclass”).

78. Excluded from the Classes are Defendants, the officers and directors of the Defendants at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which either Defendants have or had a controlling interest.

79. Plaintiff is a member of the Classes she seeks to represent.

80. The Classes are so numerous that joinder of all members is impractical. Although Plaintiff does not yet know the exact size of the Classes, it is believed that there are at least thousands of Class members.

81. The Classes are ascertainable because the Class members can be identified by objective criteria – all individuals who accessed their patient portals on www.thriveworks.com for mental health services. Individual notice can be provided to Class members “who can be identified through reasonable effort.” Fed. R. Civ. P. 23(c)(2)(B).

82. There are numerous questions of law and fact common to the Classes, which predominate over any individual actions or issues, including but not limited to:

- A. Whether Defendants gave the Class members a reasonable expectation of privacy that their information was not being shared with third parties;
- B. Whether Defendants' disclosure of information constitutes a violation of the claims asserted;
- C. Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and
- D. Whether Plaintiff and Class members have sustained damages as a result of Defendants' conduct and if so, what is the appropriate measure of damages or restitution.

83. Plaintiff's claims are typical of the claims of the members of the Classes, as all members are similarly affected by Defendants' wrongful conduct. Plaintiff has no interests antagonistic to the interests of the other members of the Class. Plaintiff and all members of the Classes have sustained economic injury arising out of Defendants' violations of law as alleged herein.

84. Plaintiff is an adequate representative of the Classes because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained counsel competent and experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and her counsel.

85. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability. Individualized litigation

increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendants' liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

86. Plaintiff reserves the right to revise the allegations and class definition based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

COUNT I

Violation of the Electronic Communications Privacy Act 18 U.S.C. § 2511(1), *et seq.*

87. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

88. Plaintiff brings this claim on behalf of herself and members of the Class.

89. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

90. The ECPA protects both the sending and the receipt of communications.

91. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

92. The transmission of Plaintiff's PII and PHI to Defendants' Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

93. The transmission of PII and PHI between Plaintiff and Class members and Defendants' Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing, ...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

94. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

95. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

96. The ECPA defines "electronic, mechanical, or other device," as "any device...which can be used to intercept a[n]...electronic communication[.]" 18 U.S.C. § 2510(5).

97. The following instruments constitute "devices" within the meaning of the ECPA:

- a. The computer codes and programs Defendants, LinkedIn, and Google used to track Plaintiff and Class members communications while they were navigating the Website;
- b. Plaintiff's and Class members' browsers;
- c. Plaintiff's and Class members' mobile devices;
- d. Defendants', LinkedIn's, and Google's web and ad servers;
- e. The plan Defendants, LinkedIn, and Google carried out to effectuate the

tracking and interception of Plaintiff's and Class members' communications while they were using a web browser to navigate the Website.

98. Plaintiff and Class members' interactions with Defendants' Website are electronic communications under the ECPA.

99. By utilizing and embedding the Tracking Technology provided by LinkedIn and Google on its Website, Defendants intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

100. Specifically, Defendants intercepted—in real time—Plaintiff's and Class members' electronic communications via the Tracking Technologies provided by LinkedIn and Google on its Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and PHI to third parties, such as LinkedIn and Google.

101. Defendants intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class members regarding PII and PHI, including their identities and information related to the mental health services they received. This confidential information is then monetized for targeted advertising purposes, among other things.

102. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(c).

103. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(d).

104. Defendants intentionally intercepted the contents of Plaintiff's and Class members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, HIPPA, the FTC Act, the VHRPA, and invasion of privacy, among others.

105. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendants violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.⁵⁰

106. Plaintiff's information that Defendants disclosed to Google qualifies as IIHI, and Defendants violated Plaintiff's and Class members' expectations of privacy. Such conduct

⁵⁰ 42 U.S.C. § 1320d-6.

constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6.

Defendants used the electronic communications to increase their profit margins. Defendants specifically used the Tracking Technologies provided by LinkedIn and Google to track and utilize Plaintiff's and Class members' PII and PHI for financial gain.

107. Similarly, the VHRPA § 31.1-127.1:03(A) codifies a patients' right to the privacy of their health records.

108. Plaintiff's and Class members' communications of their PHI to Defendants via its Website are "health records" defined under § 31.1-127.1:03(B).

109. The VHRPA provides that "except when permitted or required by this section..., no health care entity, or other person working in a health care setting, may disclose an individual's health records." § 31.1-127.1:03(A).

110. Defendants' conduct violated the VHRPA where it disclosed its patients' PHI to LinkedIn and Google without their express authorization or consent.

111. Defendants were not acting under the color of law to intercept Plaintiff's and Class members' wire or electronic communications.

112. Plaintiff and Class members did not authorize Defendants to acquire the content of their communications for purposes of invading Plaintiff's and Class members' privacy. Plaintiff and Class members, all of whom are patients of Defendants, had a reasonable expectation that Defendants would not redirect their communications to LinkedIn or Google without their knowledge or consent.

113. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq.*

114. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of \$10,000 or \$100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

COUNT II
Violation of the Pennsylvania Wiretapping Act
18 Pa. Cons. Stat. § 5701, et seq.

115. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

116. Plaintiff brings this Count individually and on behalf of the members of the Pennsylvania Subclass.

117. The Pennsylvania Wiretapping Act prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

118. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at a rate of \$100 per day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

119. "Intercept" is defined as the "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other

device.” 18 Pa. Cons. Stat. § 5702. “Electronic, mechanical or other device,” in turn, means “[a]ny device or apparatus ... that can be used to intercept a wire, electronic or oral communication[.]” *Id.*

120. The following constitutes a device within the meaning of 18 Pa. Cons. Stat. § 5702:

- a. The computer codes and programs that Defendants used to track Plaintiff and Class members’ communications while navigating the Website;
- b. Plaintiff’s and Class members’ web browsers;
- c. Plaintiff’s and Class members’ computing devices;
- d. Defendants’ web servers;
- e. The web servers from which LinkedIn and Google received the Plaintiff’s and Class members’ communications while they were using a web browser to access the Website;
- f. The plan Defendants carried out to effectuate their tracking of Plaintiff’s and Class members’ communications while using a web browser to access the Website.

121. At all relevant times, Defendants procured LinkedIn and Google to track and intercept Plaintiff’s and Class members’ internet communications while navigating the Website. They intercepted these communications without authorization and consent from Plaintiff and Class members.

122. Defendants, when procuring LinkedIn and Google to intercept Plaintiff’s communications, intended for LinkedIn and Google to learn the meaning of the content the patient requested.

123. Plaintiff and Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

124. Plaintiff and Class members were not aware that their electronic communications were being intercepted by LinkedIn and Google.

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

- a. Determining that this action is a proper class action;
- b. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Classes and naming Plaintiff's attorneys as Class Counsel to represent the Classes;
- c. For an order declaring that Defendants' conduct violates the statutes referenced herein;
- d. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;
- e. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial;
- f. Ordering Defendants to disgorge revenues and profits wrongfully obtained;
- g. For prejudgment interest on all amounts awarded;
- h. For injunctive relief ordering Defendants to immediately cease their illegal conduct;
- i. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit; and

- j. Grant Plaintiff and the Class members such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: April 25, 2025

Respectfully submitted,

By: /s/ Joshua Erlich

THE ERLICH LAW OFFICE, PLLC
Joshua Erlich, VA Bar No. 81298
1550 Wilson Blvd., Ste. 700
Arlington, VA 22201
Tel: (703) 791-9087
Fax: (703) 722-8114
Email: jerlich@erlichlawoffice.com

BURSOR & FISHER, P.A.

Alec M. Leslie (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: aleslie@bursor.com

Pro hac vice pending

BURSOR & FISHER, P.A.

Stephen A. Beck (*pro hac vice* forthcoming)
701 Brickell Ave., Suite 2100
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 676-9006
E-Mail: sbeck@bursor.com

Pro hac vice pending

Attorneys for Plaintiff